

(19)



(11)

EP 3 667 594 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:

01.06.2022 Bulletin 2022/22

(51) International Patent Classification (IPC):

G06Q 20/36 ^(2012.01) **H04L 29/06** ^(2006.01)
G06F 21/44 ^(2013.01) **G06F 21/62** ^(2013.01)

(21) Application number: **19207089.4**

(52) Cooperative Patent Classification (CPC):

G06F 21/44; G06F 21/6218; H04L 63/10

(22) Date of filing: **29.09.2014**

(54) PAPERLESS APPLICATION

PAPIERFREIE ANWENDUNG

APPLICATION SANS PAPIER

(84) Designated Contracting States:

**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

(30) Priority: **30.09.2013 US 201361884826 P**

(43) Date of publication of application:

17.06.2020 Bulletin 2020/25

(62) Document number(s) of the earlier application(s) in
accordance with Art. 76 EPC:

14846886.1 / 3 053 119

(73) Proprietor: **Fasetto, Inc.**

Scottsdale, AZ 85251 (US)

(72) Inventors:

- **MALPASS, Luke**
Staffordshire, ST5 6TB (GB)
- **CHRISTMAS, Coy**
Superior WI 54880 (US)

(74) Representative: **Hargreaves, Timothy Edward**

Marks & Clerk LLP
40 Torphichen Street
Edinburgh EH3 8JB (GB)

(56) References cited:

CN-A- 102 376 133 CN-A- 103 077 462

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

FIELD OF INVENTION

[0001] The present disclosure relates to systems, methods, and programs for processing and transmitting data between devices.

BACKGROUND

[0002] Conventional methods of transmitting information between and/or among various parties, for example from businesses to consumers, typically can require either hard copies of the information (e.g., a printed receipt) and/or may require that one of the parties manually enter information into another party's electronic system (e.g., having the customer manually type an email address) to transmit the data electronically.

[0003] Such systems, methods, and/or programs can suffer from systemic inefficiencies and risks, such as loss of time in entering in a party's information, loss of a printed receipt, increased marginal costs, loss of electronic data, subsequent downstream processing, and discouragement from using paperless communication.

[0004] CN103077462A is directed to an electronic receipt system based on a terminal, comprising a scanning module, a system barcode module, a data synchronization module, and a service logic module.

[0005] CN102376133A is directed to a paperless electronic invoice system, which comprises a mobile phone, a point-of-sale (POS) and a data processing host. The POS is provided with a bar code reading module and an electronic invoice functional module.

SUMMARY

[0006] Systems, methods, and articles of manufacture for transmitting information between devices are disclosed. A receiving device may generate a key. The key may identify a digital storage location. The key may be configured to be scanned by a transmitting device. The transmitting device may be configured to transmit information to a file management system in response to scanning the key. The receiving device may transmit a request to access the information to the file management system.

[0007] In various embodiments, a receiving device associated with a user may generate a key. The key may identify a file location associated with the user. A transmitting device may scan the key. The transmitting device may transmit information to a file management system in response to scanning the key. The file management system may store the information in the file location. The file management system may grant the user access to the information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] A more complete understanding may be de-

rived by referring to the detailed description and claims when considered in connection with the Figures, wherein like reference numbers refer to similar elements throughout the Figures, and:

FIG. 1 illustrates, in accordance with various embodiments, a system for transmitting information between devices;

FIG. 2 illustrates a receiving device generating a key in accordance with various embodiments;

FIG. 3 illustrates a transmitting device scanning a receiving device in accordance with various embodiments.

FIG. 4 illustrates a receiving device displaying received information in accordance with various embodiments.

FIG. 5 illustrates an authorization process for electronically accessing information according to various embodiments; and

FIG. 6 illustrates a process for transmitting information without a network in accordance with various embodiments.

DETAILED DESCRIPTION

[0009] The invention is disclosed by the independent claims. Further embodiments are described by the dependent claims. The detailed description of exemplary embodiments herein makes reference to the accompanying drawings and pictures, which show various embodiments by way of illustration. While these various embodiments are described in sufficient detail to enable those skilled in the art to practice the disclosure, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the scope of the disclosure. Thus, the detailed description herein is presented for purposes of illustration only and not of limitation. For example, the steps recited in any of the method or process descriptions may be executed in any order and are not limited to the order presented. Moreover, any of the functions or steps may be outsourced to or performed by one or more third parties. Furthermore, any reference to singular includes plural embodiments, and any reference to more than one component may include a singular embodiment.

[0010] Various systems, methods and computer program products are provided in this disclosure. In the detailed description herein, references to "various embodiments," "one embodiment," "an embodiment," "an example embodiment," etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such fea-

ture, structure, or characteristic in connection with other embodiments whether or not explicitly described. After reading the description, it will be apparent to one skilled in the relevant art(s) how to implement the disclosure in alternative embodiments.

[0011] Systems, methods, and programs facilitating the electronic transfer of information are disclosed according to various embodiments.

[0012] In various embodiments, a user creates an account on a framework, such as a Graphical User Interface ("GUI") described below. The account may be connected to an application which the user may install on an electronic device. The account may contain the user's specific information such as contact information and can in some embodiments be linked with a key containing linking and access data with an account, folder, and/or personal identifier. Exemplary keys can include items such as a bar code or QR code which can be displayed, for example, on the user's electronic devices (e.g., a smartphone, tablet, or personal home computer) through any means and/or software that is functional with the created account and/or known identification systems (e.g., Radio Frequency Identification (RFID)) tags.

[0013] In some embodiments, when a transfer of information is desired (e.g., from a third party in the form of a receipt for goods sold or services performed), the user can present the key and an electronic device of the transmitting party can read the key which is linked to the account containing the user's specific information. The transmitting party, by reading the key, can grant the user's associated account access to the information. In some embodiments, when a plurality of keys are read, the electronic device of the transmitting party can be set to read a plurality of keys to allow a plurality of accounts access to the information.

[0014] The information may be presented in any form or medium, and in various embodiments, the content may be delivered electronically and/or be capable of being presented electronically. For example, in various embodiments the information may comprise, but is not limited to, a receipt, a website, a uniform resource locator ("URL"), a document (e.g., a Microsoft Word document, a Microsoft Excel document, an Adobe® pdf document, etc.), an eBook, an emagazine, a receipt, an application or microapplication (as described below), an SMS or other type of text message, an email, social media sites including Facebook®, Foursquare®, Twitter®, MySpace®, LinkedIn®, and the like, and/or MMS, and combinations thereof. Additional forms of exemplary information include, but are not limited to, music (MP3, MP2, WV, etc.), videos (e.g., .mpeg, .mpg, .mov, etc.), pictures (e.g., a bitmap, jpeg, gif, png, etc.), slideshow presentations, and/or combinations thereof.

[0015] As used herein, "user" is not particularly limited and may include, for example, an individual, a plurality of individuals, a group of individuals, a business, an organization, and/or another form of recognizable entity. Additionally, as used herein, "transmitting party" is

not particularly limited and may include the user. For example, transmitting party may include a user sending information from one electronic device controlled and/or owned by the user to another electronic device controlled and/or owned by the user or, to another party.

[0016] For example, a college student wanting to send notes from his laptop to his smartphone can generate a key on the laptop, use the smartphone to scan the key from his laptop to his phone, and transfer the information from the laptop to the smartphone. As yet another example, one student could transfer notes from a college class stored on a server and/or network, such as a cloud, to another student by activating an electronic device, such as a smartphone. In this example, the student receiving the notes may generate a key, such as a barcode. The transferring student's electronic device may read the key and request the server and/or network to allow the account associated with the key to have access to the information. The server may make a copy in a designated account and/or folder assigned to the scanned key. The receiving student could then download the transmitted class notes to an authorized electronic device, such as the receiving student's smartphone or laptop.

[0017] Various embodiments can include one or more known keys which can in some embodiments act as an account and/or personal identifiers. This can in some embodiments be accomplished through registration of an account through a mobile device and/or through the Internet. In some embodiments, multiple keys can be associated with the same account and/or location and, in some embodiments, a single key or multiple keys can provide access to multiple accounts.

[0018] The accounts can be linked with various online programs and/or accounts, such as a social media site, a merchant website, an affiliate or partner websites, an external vendor, mobile device communications, and/or cloud computing. Examples of social media sites include Facebook®, Foursquare®, Twitter®, MySpace®, LinkedIn®, and the like. The accounts and/or personal identifiers can also be linked with electronic devices, such as a smartphone and/or tablet.

[0019] Examples of cloud computing include various types of systems and concepts of varying technology and paradigms. Exemplary models of cloud computing include infrastructure as a service (IaaS), platform as a service (PaaS), and/or software as a service (SaaS) models. The type of cloud is not particularly limited and can in various embodiments include public clouds, community clouds, hybrid clouds, distributed clouds. In some embodiments, the cloud can use various forms of cloud management strategies, such as user self-provisioning, advance provisioning, and/or dynamic provisioning management strategies. In various embodiments, the cloud management system is not limited and can use any currently available cloud management systems, such as systems available from HP®, Novell®, Eucalyptus®, OpenNebula®, and Citrix®.

[0020] In some embodiments, the keys can be any ap-

propriate technology which would transmit sufficient data for the application to instruct the server and/or network to associate the correct destination for the data transfer. Exemplary keys can include a barcode, a matrix (2D) barcode (e.g. a QR code, Aztec code, High Capacity Color Barcode, and PDF417), an RFID chip, information obtained from any type of fingerprint reader, audio waves, iris recognition, stored cookies, and/or digital certificates, such as internet certificates for SSL (Secure Socket Layer) and S/MIME (Secure/Multipurpose Internet Mail Extensions). The form of the key is not particularly limited, for example, the barcode or QR code could be either printed or could be presented electronically on the screen of an electronic device. Keys can also be any form of known digital identification sent via wireless communication, such as Bluetooth, infrared, radio, and other known communication methods. In some embodiments, key can be a physical object, such as a card with a magnetic strip, similar to a credit card or gift card. In other embodiments, the key can be completely electronic and can be associated with a person's electronic account, such as an Amazon® or PayPal® account.

[0021] For example, when purchasing items from an online retailer, such as Amazon®, a user could associate a key with their retail account. When purchases are made, the retailer, rather than sending an email copy confirming the purchase, may grant the user's associated account access to the information, and the information can be copied to a specified location.

[0022] In some embodiments, the access can be temporally limited (e.g., has an expiration date) and/or may have other permission restrictions by the transmitting party (e.g., read only). In some embodiments, keys can be remotely blocked by the user associated with the key and/or another party if compromised and/or for any other reason, which in some embodiments can render all previous shared content inaccessible.

[0023] After the transferring party obtains the information contained in the key, the transferring party can send the key to the server, which may grant the user access to the information to be transferred. The desired information can then be copied from the transferring party to the user.

[0024] The key can be read by any corresponding electrical device with the capability of reading the provided key. Key readers can include, for example, conventional point-of-sale systems (POS), digital cameras, smartphones, and RFID readers. For example, in some embodiments existing point-of sale systems, such as computerized barcode scanners at check-out counters can be used to read corresponding keys, such as barcodes or QR codes.

[0025] The key and reader systems can in some embodiments work together in an active system or can be passive systems. For example, the RFID key and reader system in some embodiments can be Passive Reader Active Tag (PRAT) systems, can in some embodiments be Active Reader Passive Tag (ARPT) systems, and can

in some embodiments be Active Reader Active Tag (ARAT) systems. The frequency band of the signal is not particularly limited and can, for example, range anywhere from about 120 kHz to about 10 GHz. The readers can be fixed or can be mobile.

[0026] For example, by way of illustration, if a user were to purchase a product from a local vendor, the user could present an electronic mobile device, such as a smartphone. The user could activate the associated program and could then display an associated QR code linked with the user's account connected to the associated program. The vendor could then scan the displayed associated QR code with an existing scanner containing software compatible with the associated program.

[0027] The user's account could then be granted access to the receipt information (e.g., vendor identification, sales price, quantity, identification of item purchased, and method of payment such as an account linked with a specific credit card), which could then be transmitted electronically from the vendor's data storage to the user's account.

[0028] The user, in some embodiments, can then download the transmitted information onto the mobile electronic device and/or can download uploaded transmitted information from a cloud computing network.

[0029] In the case of downloading the transmitted information from a cloud computing network, the party desiring to transmit the information (e.g., the vendor) may transmit the information to the user from a vendor specific location on a cloud to the user's specific location on a cloud where the transmitted information may be stored. The transmitted information may also be compressed to minimize the time and/or data for the transmission. In various embodiments, the transmitted information may contain links to files or other data stored on the network, rather than the actual desired information themselves.

[0030] The downloaded information can then be categorized by a program and/or application associated with the user's specific account. The program and/or application can then send the information to the appropriately associated software (e.g., financial planning software, such as QuickBooks®).

[0031] Referring to FIG. 1, a system for transmitting information between devices is illustrated according to various embodiments. The system 100 may comprise a receiving device 110, a transmitting device 120, a database 130, and a server 140. In various embodiments, the database 130 and or the server 140 may be a part of a file management system. The file management system may be configured to store information uploaded from the transmitting device 120 and the receiving device 110. The file management system may control access to the information. The various components of system 100 may communicate via a network 150. However, in various embodiments, the various components of system 100 may communicated directly without communication over the network 150, such as via Bluetooth®, NFC, a wireless chip, visual communication, or any other suitable

ble method of communication between the components of system 100. In various embodiments, the receiving device 110 may comprise a mobile electronic device, such as a smartphone.

[0032] Referring to FIG. 2, a receiving device 210 generating a key 212 is illustrated according to various embodiments. The receiving device 210 may generate a key 212 by a variety of methods. For example, a user may physically shake the receiving device 210, causing the receiving device 210 to generate the key 212. The user may tap a button, initiate an application, speak a voice command, scan a fingerprint, or instruct the receiving device 210 to generate the key by any other suitable method.

[0033] The key 212 may comprise any symbol, signal, device, or other indicia capable of identifying information. For example, as illustrated in FIG. 2, the key 212 may comprise a QR code. In various embodiments, the key 212 may uniquely identify at least one of the receiving device 210, a user of the receiving device 210, an account of the user of the mobile electronic device, or a unique digital file location. In various embodiments, the key 212 may identify a location of a digital folder in which information should be received. For example, the key 212 may identify a location in a file management system which should receive information. In various embodiments, the file management system may be a cloud computing system.

[0034] A transmitting device 220 may be configured to scan the key 212. In various embodiments, the transmitting device 220 may comprise an optical device, such as a barcode scanner, which may optically scan the key 212. However, the transmitting device 220 may receive information from the key 212 by any suitable method, such as NFC, RFID, or WIFI.

[0035] Referring, to FIG. 3, a transmitting device 320 is illustrated scanning a receiving device 310 according to various embodiments. A receiving device 310 may generate a key 312. A transmitting device 320 may scan the key 312. In various embodiments, both the transmitting device 320 and the receiving device 310 may be mobile electronic devices, such as smartphones. In various embodiments, a user of the transmitting device may initiate an application in order to scan the key 312. In response to scanning the key 312, the transmitting device 320 may transmit desired information, such as a receipt, to an electronic account associated with the receiving device 310 and/or a user of the receiving device 310. In various embodiments, the transmitting device 320 may compress the information prior to transmitting the information. In various embodiments, the transmitting device 320 may transmit the information directly to the receiving device 310 without using a network. Examples of such transmission in Bluetooth® transmission. In another embodiment, a transport layer such as the Arch® transport layer available from Fasetto, LLC may be used. For more information regarding the Arch® transport layer, see U.S. Patent Application Serial No. 14/164,919 entitled "SYS-

TEMS AND METHODS FOR PEER TO PEER COMMUNICATION," and filed on January 27, 2014.

[0036] Referring to FIG. 4, the receiving device 310 may download the compressed information sent to the electronic account associated with the receiving device 310 onto the receiving device 310. The receiving device 310 may decompress the compressed information and display the information transmitted in a graphical user interface on display screen 314. For example, the receiving device 310 may display a receipt for a purchase made from the user of the transmitting device 320.

[0037] Referring to FIG. 5, an authorization process for electronically accessing information is illustrated according to various embodiments. A key corresponding to an account or electronic folder is activated (step 510). A key may be activated in various ways depending on the type of key and is not particularly limited. For example, in some embodiments a key may be activated by shaking an electronic device, or in some embodiments may be activated in the form of swiping a card similar to a credit card containing a magnetic strip.

[0038] The account, folder, and/or personal identifier with which the key is associated are not particularly limited. In some embodiments, the user can designate and create accounts and/or folders to receive certain types of information. For example, the user may designate a first folder to receive fuel receipts and a second folder to receive restaurant receipts. In some embodiments, the key may identify the particular folder which should receive a receipt or other information. In some embodiments, folders can be default folders created by a program. In some embodiments, the key can be associated with several folders for storage and/or processing by a single or plurality of programs and/or applications. For example, a folder can be associated with the types of information transmitted (e.g., videos, music, documents, pictures, etc.).

[0039] An electronic device may read the key (step 520). The electronic device may comprise a point of sale device, a smartphone, an RFID reader, or any other suitable device capable of reading the key.

[0040] Then, the authentication is guarded (step 530). For example, in some embodiments, a random number can be generated and/or assigned to the specific information and/or user. This number, which can form part of the information contained in the key, can be stored, for example, on a server as a set of instructions in a database. Thus, the location of the information can, in some embodiments, avoid being disclosed and/or can provide additional security measures. For example, in some embodiments, when the key expires and/or is revoked, the server will inform a user trying to access the no longer authorized information that the key is no longer valid. Also, in some embodiments, the server can track usage based on the assigned random number contained in a key. For example, in some embodiments, (e.g., when the server is informed to grant access to the data referred to in the key), the server can track and/or monitor the use

of the information (e.g., attempts access, times copied, identity of authorized users, time of access, location, times viewed, edits to information, and/or other information associated with a file or data history).

[0041] In some embodiments, such as embodiments which do not require being online, the authentication and guarding can be done via the transmitting party's device prior to transmission, for example a direct transfer method. Here, the transmitting party can be asked if they would like to send the file to the user requesting access to the information over a local area. In some embodiments, a random and/or one time use number can be included in the key. This can allow for the transmitting party to be able to ensure the identity of the user. For example, in some cases the transmitting party and the user are in close physical proximity and the transmitting party can physically be aware of to whom they are granting access.

[0042] The information can be stored on an electronic device (e.g., on a hard drive) or can in some embodiments, be stored on a network, on the internet, and/or in a cloud. In some embodiments, the account associated with the key can identify the associated account and gain access to the information be transferred, viewed, and/or copied.

[0043] In various embodiments, the location for the storage of the transferred information associated with the key can be set prior to activation, can be assigned at the moment of activation, and/or can be assigned after authorization is given. The location associated with the key can be manually or automatically assigned. For example, a program could automatically associate a folder within an assigned account based on the type of information being transmitted and/or could be associated based on the movement of an electronic device assigned to a specific account and/or folder.

[0044] For example, if gas were purchased from a vendor, access could be transmitted to a specific user account associated with a key and/or could go to a specific folder (e.g., an expense account for business) and/or could be automatically associated with a specific subfolder within a folder (e.g., a gas expense account). The key (e.g., a matrix (2D) code) could be read, for example, from an appropriate POS device (e.g., a conventional scanner) during checkout. The specific location can be manually assigned by the user or can automatically be assigned based on the type of information being transferred. For example, the vendor could automatically designate the information that it transmits based on its products and/or services. In some embodiments, this classification can be automatically be designated through existing classifications systems, such as standard industrial classification, such as North American Industry Classification System (NAICS).

[0045] In some embodiments, information, such as a receipt, can be accompanied by additional information provided by a transferring party. For example, a law firm providing a final draft of a contract could include in the transferred information both the contract as well as a bill

for the legal services rendered. In some embodiments, the access granted need not be in a single location (e.g., in the same file on a server). Using the previous example, the bill for legal services could be kept in a different location than the final draft of the contract.

[0046] Furthermore, in some embodiments, when there is insufficient data from the transferring electronic device to properly associate the information with the correct destination within an account (e.g., when only a picture of a receipt is available), the information may be processed to determine the correct destination with an account using various known methods (e.g., optical character recognition (OCR) and/or intelligent character recognition (ICR)).

[0047] Additionally, in some embodiments, even when the information can be properly associated with the correct destination within an account, the information can be processed to facilitate use of the transferred information by a user and/or other programs and/or applications. For example, the information could be processed into a comma-separated values (CSV) file to facilitate use in consumer, business, and scientific programs and/or applications.

[0048] Access may be granted to the information (step 540). The receiving device may transmit a request to a file management system to access the information. In various embodiments, the user may enter login credentials, such as a user name and password in order to access the information. In various embodiments, the receiving device may provide the key or the random number generated as part of the key in order to access the information.

[0049] The information may be transferred and/or copied to an account and/or electronic device associated with the key (step 550). In some embodiments, the transfer of information can occur when the account associated with the key tells the server to send the information to the chosen account and/or associated folder.

[0050] For example, the scanning of the key could give the assigned account access to the information stored by the vendor (e.g., the customer's receipt). This could, in some embodiments, based on the information, default parameters, and/or parameters set by the user, be placed in a specific location (e.g., an expense account folder). Thus, it may be possible in some embodiments to avoid associated costs of printing and scanning receipts as well as downstream processing of the information.

[0051] FIG. 6 illustrates a process 600 for the access and/or transfer of electronically stored data when a traditional public network, such as a digital mobile network, is not available. First, a transmitting device may connect to a receiving device (step 610). For example, the two devices can be connected via known communication methods, such as by creating WLAN or a hot spot with Bluetooth, Wi-Fi (e.g., 802.1x), NFC, audio, and/or visual transmissions or the Arch[®] transport layer as noted above. In some embodiments, the network need not be broadcasting (e.g., the WLAN may not be broadcasting

an SSID). In some embodiments, the key can simultaneously provide the SSID as well as any other required information to connect to the WLAN (e.g., a password).

[0052] The key of the receiving device is activated (step 620). A key may be activated in various ways depending on the type of key and is not particularly limited throughout this disclosure and the various embodiments exemplified herein.

[0053] The transmitting electronic device reads the key (step 630). The authentication may be guarded (step 640) (e.g., by requesting confirmation from the transmitting party to allow the use of an associated randomly generated number to access the information). In some embodiments, the key can limit the number of times the information is accessed and/or the random number is used to help protect the information and/or connected electronic devices. For example, by guarding the authentication by confirming authorization from the transmitting party with a random generated one-time use number, the actual location of the information on the transmitting device can be prevented from being disclosed and repeated attempts by a user to access information on the transmitting device can be prevented. Thus, in some embodiments, the transmitting party can protect the information and can provide improved security between electronic devices. In some embodiments, the transmitting electronic device can track and/or monitor the use of the information (e.g., access, times copied, identity of authorized users, time of access, location, times viewed, edits to information, and/or other information associated with a file or data history).

[0054] Access to the information can then be granted (step 650), which in some embodiments is stored on the transmitting electronic device. As stated above, the access granted can, in some embodiments, be associated with a one-time use permit and/or can have other access limitations which can be modified by the transmitting party.

[0055] In some embodiments, the electronic information is copied and/or transferred from a transmitting electronic device to a receiving electronic device (step 660). In some embodiments, the receiving device is granted access to the information and then that information is transferred and/or copied by the receiving electronic device into a specific location. The methods of transferring information can be any of the forms of communication with electronic devices disclosed herein.

[0056] Thereafter, the connection between the at least two electronic devices can be, in some embodiments, terminated (step 670).

[0057] Some embodiments of the present disclosure relate to systems, methods, and programs of processing and transmitting information capable of interacting in conjunction with graphical user interfaces ("GUI"), and more particularly cubic GUIs. For example, the information being transmitted may be a three-dimensional representation of a plurality of files, or the information being transmitted may be stored on a face of a cubic file. For more

information regarding cubic GUIs and three dimensional files, see U.S. Patent Application Serial No. 14/197,517 entitled "SYSTEM AND METHOD FOR CUBIC GRAPHICAL INTERFACES," and filed on March 5, 2014.

[0058] The various parties discussed herein may communicate with the network 150 via a web client. A web client may include any device (e.g., personal computer) which communicates via any network, for example such as those discussed herein. Web client may include browser applications comprising Internet browsing software installed within a computing unit or a system to conduct online transactions and/or communications. These computing units or systems may take the form of a computer or set of computers, although other types of computing units or systems may be used, including laptops, notebooks, tablets, hand held computers, personal digital assistants, set-top boxes, workstations, computer servers, main frame computers, mini-computers, PC servers, pervasive computers, network sets of computers, personal computers, such as iPads, iMACs, and MacBooks, kiosks, terminals, point of sale (POS) devices and/or terminals, televisions, or any other device capable of receiving data over a network. A web-client may run Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, or any other of the myriad software packages available for browsing the internet.

[0059] Practitioners will appreciate that a web client may or may not be in direct contact with an application server. For example, a web client may access the services of an application server through another server and/or hardware component, which may have a direct or indirect connection to an Internet server. For example, a web client may communicate with an application server via a load balancer. In various embodiments, access is through a network or the Internet through a commercially-available web-browser software package.

[0060] As those skilled in the art will appreciate, a web client may include but is not limited to an operating system (e.g., Windows NT, 95/98/2000/CE/Mobile, OS2, UNIX, Linux, Solaris, MacOS, PalmOS, etc.) as well as various conventional support software and drivers typically associated with computers. A web client may include but is not limited to any suitable personal computer, network computer, workstation, personal digital assistant, cellular phone, smartphone, minicomputer, main-frame or the like. A web client can be in a home or business environment with access to a network. In various embodiments, access is through a network or the Internet through a commercially available web-browser software package. A web client may implement security protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS). A web client may implement several application layer protocols including http, https, ftp, and sftp.

[0061] A network may include any cloud, cloud computing system or electronic communications system or method which incorporates hardware and/or software components. Communication among the parties may be

accomplished through any suitable communication channels, such as, for example, a telephone network, an extranet, an intranet, Internet, point of interaction device (point of sale device, personal digital assistant (e.g., iPhone®, Palm Pilot®, Blackberry®, cellular phone, kiosk, etc.), online communications, satellite communications, off-line communications, wireless communications, transponder communications, local area network (LAN), wide area network (WAN), virtual private network (VPN), networked or linked devices, keyboard, mouse and/or any suitable communication or data input modality. Moreover, although the system is frequently described herein as being implemented with TCP/IP communications protocols, the system may also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI, any tunneling protocol (e.g. IPsec, SSH), or any number of existing or future protocols. If the network is in the nature of a public network, such as the Internet, it may be advantageous to presume the network to be insecure and open to eavesdroppers. Specific information related to the protocols, standards, and application software utilized in connection with the Internet is generally known to those skilled in the art and, as such, need not be detailed herein. See, for example, DILIP NAIK, INTERNET STANDARDS AND PROTOCOLS (1998); JAVA 2 COMPLETE, various authors, (Sybex 1999); DEBORAH RAY AND ERIC RAY, MASTERING HTML 4.0 (1997); and LOSHIN, TCP/IP CLEARLY EXPLAINED (1997) and DAVID GOURLEY AND BRIAN TOTTY, HTTP, THE DEFINITIVE GUIDE (2002).

[0062] The various system components may be independently, separately or collectively suitably coupled to the network via data links which includes, for example, a connection to an Internet Service Provider (ISP) over the local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Line (DSL), or various wireless communication methods, see, e.g., GILBERT HELD, UNDERSTANDING DATA COMMUNICATIONS (1996). It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network. Moreover, the system contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

[0063] Any communication, transmission and/or channel discussed herein may include any system or method for delivering content (e.g. data, information, metadata, etc.), and/or the content itself. The content may be presented in any form or medium, and in various embodiments, the content may be delivered electronically and/or capable of being presented electronically. For example, a channel may comprise a website, a uniform resource locator ("URL"), a document (e.g., a Microsoft Word document, a Microsoft Excel document, an Adobe .pdf document, etc.), an "eBook," an "emagazine," an application or microapplication (as described below), an SMS or other type of text message, an email, social media (e.g.,

Facebook®, Foursquare®, Twitter®, MySpace®, LinkedIn®, and the like), MMS and/or other type of communication technology. In various embodiments, a channel may be hosted or provided by a data partner. In various embodiments, the distribution channel may comprise at least one of a merchant website, a social media website, affiliate or partner websites, an external vendor, a mobile device communication, social media network and/or location based service. Distribution channels may include at least one of a merchant website, a social media site, affiliate or partner websites, an external vendor, and a mobile device communication. Examples of social media sites include Facebook®, foursquare®, Twitter®, MySpace®, LinkedIn®, and the like. Moreover, examples of mobile device communications include texting, email, and mobile applications for smartphones.

[0064] In various embodiments, the methods described herein are implemented using the various particular machines described herein. The methods described herein may be implemented using the below particular machines, and those hereinafter developed, in any suitable combination, as would be appreciated immediately by one skilled in the art. Further, as is unambiguous from this disclosure, the methods described herein may result in various transformations of certain articles.

[0065] For the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical system.

[0066] The various system components discussed herein may include one or more of the following: a host server or other computing systems including a processor for processing digital data; a memory coupled to the processor for storing digital data; an input digitizer coupled to the processor for inputting digital data; an application program stored in the memory and accessible by the processor for directing processing of digital data by the processor; a display device coupled to the processor and memory for displaying information derived from digital data processed by the processor; and a plurality of databases. Various databases used herein may include: client data; merchant data; financial institution data; and/or like data useful in the operation of the system. As those skilled in the art will appreciate, user computer may include an operating system (e.g., Windows NT, Windows 95/98/2000, Windows XP, Windows Vista, Windows 7, OS2, UNIX, Linux, Solaris, MacOS, etc.) as well as various conventional support software and drivers typically associated with computers.

[0067] The present system or any part(s) or function(s) thereof may be implemented using hardware, software

or a combination thereof and may be implemented in one or more computer systems or other processing systems. However, the manipulations performed by embodiments were often referred to in terms, such as matching or selecting, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein. Rather, the operations may be machine operations. Useful machines for performing the various embodiments include general purpose digital computers or similar devices.

[0068] In fact, in various embodiments, the embodiments are directed toward one or more computer systems capable of carrying out the functionality described herein. The computer system includes one or more processors. The processor is connected to a communication infrastructure (e.g., a communications bus, cross over bar, or network). Various software embodiments are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art(s) how to implement various embodiments using other computer systems and/or architectures. Computer system can include a display interface that forwards graphics, text, and other data from the communication infrastructure (or from a frame buffer not shown) for display on a display unit.

[0069] Computer system also includes a main memory, such as for example random access memory (RAM), and may also include a secondary memory. The secondary memory may include, for example, a hard disk drive and/or a removable storage drive, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive reads from and/or writes to a removable storage unit in a well-known manner. Removable storage unit represents a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive. As will be appreciated, the removable storage unit includes a computer usable storage medium having stored therein computer software and/or data.

[0070] In various embodiments, secondary memory may include other similar devices for allowing computer programs or other instructions to be loaded into computer system. Such devices may include, for example, a removable storage unit and an interface. Examples of such may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an erasable programmable read only memory (EPROM), or programmable read only memory (PROM)) and associated socket, and other removable storage units and interfaces, which allow software and data to be transferred from the removable storage unit to computer system.

[0071] Computer system may also include a communications interface. Communications interface allows software and data to be transferred between computer system and external devices. Examples of communica-

tions interface may include a modem, a network interface (such as an Ethernet card), a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communications interface are in the form of signals which may be electronic, electromagnetic, optical or other signals capable of being received by communications interface. These signals are provided to communications interface via a communications path (e.g., channel). This channel carries signals and may be implemented using wire, cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, wireless and other communications channels.

[0072] The terms "computer program medium" and "computer usable medium" are used to generally refer to media such as removable storage drive and a hard disk installed in hard disk drive. These computer program products provide software to computer system.

[0073] Computer programs (also referred to as computer control logic) are stored in main memory and/or secondary memory. Computer programs may also be received via communications interface. Such computer programs, when executed, enable the computer system to perform the features as discussed herein. In particular, the computer programs, when executed, enable the processor to perform the features of various embodiments. Accordingly, such computer programs represent controllers of the computer system.

[0074] In various embodiments, software may be stored in a computer program product and loaded into computer system using removable storage drive, hard disk drive or communications interface. The control logic (software), when executed by the processor, causes the processor to perform the functions of various embodiments as described herein. In various embodiments, hardware components such as application specific integrated circuits (ASICs). Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s). **[0079a]** In various embodiments, the server may include application servers (e.g. WEB SPHERE, WEB LOGIC, JBOSS). In various embodiments, the server may include web servers (e.g. APACHE, IIS, GWS, SUN JAVA SYSTEM WEB SERVER).

[0075] In various embodiments, components, modules, and/or engines of system 700 may be implemented as micro-applications or micro-apps. Micro-apps are typically deployed in the context of a mobile operating system, including for example, a Palm mobile operating system, a Windows mobile operating system, an Android Operating System, Apple iOS, a Blackberry operating system and the like. The micro-app may be configured to leverage the resources of the larger operating system and associated hardware via a set of predetermined rules which govern the operations of various operating systems and hardware resources. For example, where a micro-app desires to communicate with a device or network other than the mobile device or mobile operating system,

the micro-app may leverage the communication protocol of the operating system and associated device hardware under the predetermined rules of the mobile operating system. Moreover, where the micro-app desires an input from a user, the micro-app may be configured to request a response from the operating system which monitors various hardware components and then communicates a detected input from the hardware to the micro-app.

[0076] "Cloud" or "Cloud computing" includes a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing may include location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand. For more information regarding cloud computing, see the NIST's (National Institute of Standards and Technology) definition of cloud computing at <http://cs-rc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc> (last visited February 4, 2011).

[0077] As used herein, "transmit" may include sending electronic data from one system component to another over a network connection. Additionally, as used herein, "data" may include encompassing information such as commands, queries, files, data for storage, and the like in digital or any other form.

[0078] The system contemplates uses in association with web services, utility computing, pervasive and individualized computing, security and identity solutions, autonomic computing, cloud computing, commodity computing, mobility and wireless solutions, open source, biometrics, grid computing and/or mesh computing.

[0079] Any databases discussed herein may include relational, hierarchical, graphical, or object-oriented structure and/or any other database configurations. Common database products that may be used to implement the databases include DB2 by IBM (Armonk, NY), various database products available from Oracle Corporation (Redwood Shores, CA), Microsoft Access or Microsoft SQL Server by Microsoft Corporation (Redmond, Washington), MySQL by MySQL AB (Uppsala, Sweden), or any other suitable database product. Moreover, the databases may be organized in any suitable manner, for example, as data tables or lookup tables. Each record may be a single file, a series of files, a linked series of data fields or any other data structure. Association of certain data may be accomplished through any desired data association technique such as those known or practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, using a key field in the tables to speed searches, sequential searches through all the tables and files, sorting records in the file according to a known order to simplify lookup, and/or the like. The association step may be ac-

complished by a database merge function, for example, using a "key field" in preselected databases or data sectors. Various database tuning steps are contemplated to optimize database performance. For example, frequently used files such as indexes may be placed on separate file systems to reduce In/Out ("I/O") bottlenecks.

[0080] More particularly, a "key field" partitions the database according to the high-level class of objects defined by the key field. For example, certain types of data may be designated as a key field in a plurality of related data tables and the data tables may then be linked on the basis of the type of data in the key field. The data corresponding to the key field in each of the linked data tables is preferably the same or of the same type. However, data tables having similar, though not identical, data in the key fields may also be linked by using AGREP, for example. In accordance with various embodiments, any suitable data storage technique may be utilized to store data without a standard format. Data sets may be stored using any suitable technique, including, for example, storing individual files using an ISO/IEC 7816-4 file structure; implementing a domain whereby a dedicated file is selected that exposes one or more elementary files containing one or more data sets; using data sets stored in individual files using a hierarchical filing system; data sets stored as records in a single file (including compression, SQL accessible, hashed via one or more keys, numeric, alphabetical by first tuple, etc.); Binary Large Object (BLOB); stored as ungrouped data elements encoded using ISO/IEC 7816-6 data elements; stored as ungrouped data elements encoded using ISO/IEC Abstract Syntax Notation (ASN.1) as in ISO/IEC 8824 and 8825; and/or other proprietary techniques that may include fractal compression methods, image compression methods, etc.

[0081] In various embodiments, the ability to store a wide variety of information in different formats is facilitated by storing the information as a BLOB. Thus, any binary information can be stored in a storage space associated with a data set. As discussed above, the binary information may be stored on the financial transaction instrument or external to but affiliated with the financial transaction instrument. The BLOB method may store data sets as ungrouped data elements formatted as a block of binary via a fixed memory offset using either fixed storage allocation, circular queue techniques, or best practices with respect to memory management (e.g., paged memory, least recently used, etc.). By using BLOB methods, the ability to store various data sets that have different formats facilitates the storage of data associated with the financial transaction instrument by multiple and unrelated owners of the data sets. For example, a first data set which may be stored may be provided by a first party, a second data set which may be stored may be provided by an unrelated second party, and yet a third data set which may be stored, may be provided by a third party unrelated to the first and second party. Each of these three exemplary data sets may contain different informa-

tion that is stored using different data storage formats and/or techniques. Further, each data set may contain subsets of data that also may be distinct from other subsets.

[0082] As stated above, in various embodiments, the data can be stored without regard to a common format. However, in various embodiments, the data set (e.g., BLOB) may be annotated in a standard manner when provided for manipulating the data onto the financial transaction instrument. The annotation may comprise a short header, trailer, or other appropriate indicator related to each data set that is configured to convey information useful in managing the various data sets. For example, the annotation may be called a "condition header," "header," "trailer," or "status," herein, and may comprise an indication of the status of the data set or may include an identifier correlated to a specific issuer or owner of the data. In one example, the first three bytes of each data set BLOB may be configured or configurable to indicate the status of that particular data set; e.g., LOADED, INITIALIZED, READY, BLOCKED, REMOVABLE, or DELETED. Subsequent bytes of data may be used to indicate for example, the identity of the issuer, user, transaction/membership account identifier or the like. Each of these condition annotations are further discussed herein.

[0083] The data set annotation may also be used for other types of status information as well as various other purposes. For example, the data set annotation may include security information establishing access levels. The access levels may, for example, be configured to permit only certain individuals, levels of employees, companies, or other entities to access data sets, or to permit access to specific data sets based on the transaction, merchant, issuer, user or the like. Furthermore, the security information may restrict/permit only certain actions such as accessing, modifying, and/or deleting data sets. In one example, the data set annotation indicates that only the data set owner or the user are permitted to delete a data set, various identified users may be permitted to access the data set for reading, and others are altogether excluded from accessing the data set. However, other access restriction parameters may also be used allowing various entities to access a data set with various permission levels as appropriate.

[0084] The data, including the header or trailer may be received by a standalone interaction device configured to add, delete, modify, or augment the data in accordance with the header or trailer. As such, in various embodiments, the header or trailer is not stored on the transaction device along with the associated issuer-owned data but instead the appropriate action may be taken by providing to the transaction instrument user at the standalone device, the appropriate option for the action to be taken. The system may contemplate a data storage arrangement wherein the header or trailer, or header or trailer history, of the data is stored on the transaction instrument in relation to the appropriate data.

[0085] One skilled in the art will also appreciate that,

for security reasons, any databases, systems, devices, servers or other components of the system may consist of any combination thereof at a single location or at multiple locations, wherein each database or system includes any of various suitable security features, such as firewalls, access codes, encryption, decryption, compression, decompression, and/or the like. [090a] Encryption may be performed by way of any of the techniques now available in the art or which may become available—e.g., Twofish, RSA, El Gamal, Schorr signature, DSA, PGP, PKI, GPG (GnuPG), and symmetric and asymmetric cryptosystems.

[0086] The computing unit of the web client may be further equipped with an Internet browser connected to the Internet or an intranet using standard dial-up, cable, DSL or any other Internet protocol known in the art. Transactions originating at a web client may pass through a firewall in order to prevent unauthorized access from users of other networks. Further, additional firewalls may be deployed between the varying components of ACS to further enhance security.

[0087] The computers discussed herein may provide a suitable website or other Internet-based graphical user interface which is accessible by users. In various embodiments, the Microsoft Internet Information Server (IIS), Microsoft Transaction Server (MTS), and Microsoft SQL Server, are used in conjunction with the Microsoft operating system, Microsoft NT web server software, a Microsoft SQL Server database system, and a Microsoft Commerce Server. Additionally, components such as Access or Microsoft SQL Server, Oracle, Sybase, Informix MySQL, Interbase, etc., may be used to provide an Active Data Object (ADO) compliant database management system. In various embodiments, the Apache web server is used in conjunction with a Linux operating system, a MySQL database, and the Perl, PHP, and/or Python programming languages.

[0088] Any of the communications, inputs, storage, databases or displays discussed herein may be facilitated through a website having web pages. The term "web page" as it is used herein is not meant to limit the type of documents and applications that might be used to interact with the user. For example, a typical website might include, in addition to standard HTML documents, various forms, Java applets, JavaScript, active server pages (ASP), common gateway interface scripts (CGI), extensible markup language (XML), dynamic HTML, cascading style sheets (CSS), AJAX (Asynchronous Javascript And XML), helper applications, plug-ins, and the like. A server may include a web service that receives a request from a web server, the request including a URL (<http://yahoo.com/stockquotes/ge>) and an IP address (123.56.789.234). The web server retrieves the appropriate web pages and sends the data or applications for the web pages to the IP address. Web services are applications that are capable of interacting with other applications over a communications means, such as the internet. Web services are typically based on standards

or protocols such as XML, SOAP, AJAX, WSDL and UDDI. Web services methods are well known in the art, and are covered in many standard texts. See, e.g., ALEX NGHIEM, IT WEB SERVICES: A ROADMAP FOR THE ENTERPRISE (2003).

[0089] Middleware may include any hardware and/or software suitably configured to facilitate communications and/or process transactions between disparate computing systems. Middleware components are commercially available and known in the art. Middleware may be implemented through commercially available hardware and/or software, through custom hardware and/or software components, or through a combination thereof. Middleware may reside in a variety of configurations and may exist as a standalone system or may be a software component residing on the Internet server. Middleware may be configured to process transactions between the various components of an application server and any number of internal or external systems for any of the purposes disclosed herein. WebSphere MQTM (formerly MQScrics) by IBM, Inc. (Armonk, NY) is an example of a commercially available middleware product. An Enterprise Service Bus ("ESB") application is another example of middleware.

[0090] Practitioners will also appreciate that there are a number of methods for displaying data within a browser-based document. Data may be represented as standard text or within a fixed list, scrollable list, drop-down list, editable text field, fixed text field, pop-up window, and the like. Likewise, there are a number of methods available for modifying data in a web page such as, for example, free text entry using a keyboard, selection of menu items, check boxes, option boxes, and the like.

[0091] The system and method may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the system may employ various integrated circuit components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the system may be implemented with any programming or scripting language such as C, C++, C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Microsoft Active Server Pages, assembly, PERL, PHP, awk, Python, Visual Basic, SQL Stored Procedures, PL/SQL, any UNIX shell script, and extensible markup language (XML) with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the system may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. Still further, the system could be used to detect or prevent se-

curity issues with a client-side scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography and network security, see any of the following references: (1) "Applied Cryptography: Protocols, Algorithms, And Source Code In C," by Bruce Schneier, published by John Wiley & Sons (second edition, 1995); (2) "Java Cryptography" by Jonathan Knudson, published by O'Reilly & Associates (1998); (3) "Cryptography & Network Security: Principles & Practice" by William Stallings, published by Prentice Hall.

[0092] As will be appreciated by one of ordinary skill in the art, the system may be embodied as a customization of an existing system, an add-on product, a processing apparatus executing upgraded software, a standalone system, a distributed system, a method, a data processing system, a device for data processing, and/or a computer program product. Accordingly, any portion of the system or a module may take the form of a processing apparatus executing code, an internet based embodiment, an entirely hardware embodiment, or an embodiment combining aspects of the internet, software and hardware. Furthermore, the system may take the form of a computer program product on a computer-readable storage medium having computer-readable program code means embodied in the storage medium. Any suitable computer-readable storage medium may be utilized, including hard disks, CD-ROM, optical storage devices, magnetic storage devices, and/or the like.

[0093] The system and method is described herein with reference to screen shots, block diagrams and flowchart illustrations of methods, apparatus (e.g., systems), and computer program products according to various embodiments. It will be understood that each functional block of the block diagrams and the flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by computer program instructions.

[0094] These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions that execute on the computer or other programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks. These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable appa-

ratus provide steps for implementing the functions specified in the flowchart block or blocks.

[0095] Accordingly, functional blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps for performing the specified functions, and program instruction means for performing the specified functions. It will also be understood that each functional block of the block diagrams and flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, can be implemented by either special purpose hardware-based computer systems which perform the specified functions or steps, or suitable combinations of special purpose hardware and computer instructions. Further, illustrations of the process flows and the descriptions thereof may make reference to user windows, webpages, websites, web forms, prompts, etc. Practitioners will appreciate that the illustrated steps described herein may comprise in any number of configurations including the use of windows, webpages, web forms, popup windows, prompts and the like. It should be further appreciated that the multiple steps as illustrated and described may be combined into single webpages and/or windows but have been expanded for the sake of simplicity. In other cases, steps illustrated and described as single process steps may be separated into multiple webpages and/or windows but have been combined for simplicity.

[0096] The term "non-transitory" is to be understood to remove only propagating transitory signals per se from the claim scope and does not relinquish rights to all standard computer-readable media that are not only propagating transitory signals per se. Stated another way, the meaning of the term "non-transitory computer-readable medium" and "non-transitory computer-readable storage medium" should be construed to exclude only those types of transitory computer-readable media which were found in *In Re Nuijten* to fall outside the scope of patentable subject matter under 35 U.S.C. § 101.

[0097] For the purposes of this specification and appended claims, unless otherwise indicated, all numbers expressing quantities, percentages or proportions, and other numerical values used in the specification and claims, are to be understood as being modified in all instances by the term "about." Accordingly, unless indicated to the contrary, the numerical parameters set forth in the following specification and attached claims are approximations that may vary depending upon the desired properties sought to be obtained by the present invention. At the very least, and not as an attempt to limit the application of the doctrine of equivalents to the scope of the claims, each numerical parameter should at least be construed in light of the number of reported significant digits and by applying ordinary rounding techniques.

[0098] Notwithstanding that the numerical ranges and parameters setting forth the broad scope of the disclosure are approximations, the numerical values set forth in the specific examples are reported as precisely as pos-

sible. Any numerical value, however, inherently contains certain errors necessarily resulting from the standard deviation found in their respective testing measurements. Moreover, all ranges disclosed herein are to be understood to encompass any and all subranges subsumed therein. For example, a range of "less than 10" includes any and all subranges between (and including) the minimum value of zero and the maximum value of 10, that is, any and all subranges having a minimum value of equal to or greater than zero and a maximum value of equal to or less than 10, e.g., 1 to 5.

[0099] Then, in various embodiments, the user's account can then classify the transmitted information, associate the information received with additional user selected specific program, send the information to the user's selected program, and/or store the transmitted information into a specific user selected storage folder.

[0100] Benefits, other advantages, and solutions to problems have been described herein with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any elements that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of the disclosure. Reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more." Moreover, where a phrase similar to 'at least one of A, B, and C' or 'at least one of A, B, or C' is used in the claims or specification, it is intended that the phrase be interpreted to mean that A alone may be present in an embodiment, B alone may be present in an embodiment, C alone may be present in an embodiment, or that any combination of the elements A, B and C may be present in a single embodiment; for example, A and B, A and C, B and C, or A and B and C. Although the disclosure includes a method, it is contemplated that it may be embodied as computer program instructions on a tangible computer-readable carrier, such as a magnetic or optical memory or a magnetic or optical disk. All structural, chemical, and functional equivalents to the elements of the above-described exemplary embodiments that are known to those of ordinary skill in the art are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present disclosure, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. As used herein, the terms "comprises," "comprising," or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus.

Claims**1.** A method comprising:

creating, by a consumer device, a digital folder based on an expense classification in a file management system;
 generating, by the consumer device, a key (212, 312) for a transaction, wherein the key (212, 312) comprises a randomly generated number associated on a one-to-one basis with the digital folder;
 displaying, by the consumer device, the key (212, 312) on a screen of the consumer device;
 transmitting, by the consumer device, the key (212, 312) for a transaction to a receiving device (110, 210, 310);
 transmitting, by the consumer device, the randomly generated number to the file management system; and
 instructing, by the consumer device and via the file management system, a merchant device to transmit a receipt to the digital folder;
 wherein the merchant device scans the key (212, 312) displayed on the screen of the consumer device; and
 wherein, in response to the merchant device scanning the key (212, 312), the merchant device is configured to transmit the receipt to the digital folder based on an expense classification of the receipt matching the expense classification of the digital folder.

2. The method of claim 1, wherein the key (212, 312) comprises at least one of a matrix barcode or a barcode.

3. The method of claim 1, further comprising transmitting, by the consumer device, a request to access the receipt to the file management system.

4. The method of claim 3, wherein the request includes the randomly generated number.

5. The method of claim 1, further comprising displaying, by the consumer device, the receipt on the screen of the consumer device.

6. The method of claim 1, wherein the file management system comprises a cloud computing system.

7. A system comprising:

a processor in a consumer device,
 a tangible, non-transitory memory configured to communicate with the processor,
 the tangible, non-transitory memory having instructions stored thereon that, in response to ex-

ecution by the processor, cause the processor to perform operations comprising:

creating, by the consumer device, a digital folder based on an expense classification in a file management system;
 generating, by the consumer device, a key (212, 312) for a transaction, wherein the key (212, 312) comprises a randomly generated number associated on a one-to-one basis with the digital folder;
 displaying, by the consumer device, the key (212, 312) on a screen of the consumer device;
 transmitting, by the consumer device, the key (212, 312) for a transaction to a receiving device;
 transmitting, by the consumer device, the randomly generated number to the file management system; and
 instructing, by the consumer device and via the file management system, a merchant device to transmit a receipt to the digital folder;
 wherein the merchant device scans the key (212, 312) displayed on the screen of the consumer device; and
 wherein, in response to the merchant device scanning the key (212, 312), the merchant device is configured to transmit the receipt to the digital folder based on an expense classification of the receipt matching the expense classification of the digital folder.

8. The system of claim 7, wherein the key (212, 312) comprises at least one of a matrix barcode or a barcode.

9. The system of claim 7, the operations further comprising transmitting, by the consumer device, a request to access the receipt to the file management system.

10. The system of claim 9, wherein the request includes the randomly generated number.

11. The system of claim 7, the operations further comprising displaying, by the consumer device, the receipt on the screen of the consumer device.

12. The system of claim 7, wherein the file management system comprises a cloud computing system.

13. An article of manufacture including a non-transitory, tangible computer readable storage medium having instructions stored thereon that, in response to execution by a consumer device, cause the consumer

device to perform operations comprising:

creating, by the consumer device, a digital folder based on an expense classification in a file management system;
 generating, by the consumer device, a key (212, 312) for a transaction, wherein the key (212, 312) comprises a randomly generated number associated on a one-to-one basis with the digital folder;
 displaying, by the consumer device, the key (212, 312) on a screen of the consumer device;
 transmitting, by the consumer device, the key (212, 312) for a transaction to a receiving device;
 transmitting, by the consumer device, the randomly generated number to the file management system; and
 instructing, by the consumer device and via the file management system, a merchant device to transmit a receipt to the digital folder;
 wherein the merchant device scans the key (212, 312) displayed on the screen of the consumer device; and
 wherein, in response to the merchant device scanning the key (212, 312), the merchant device is configured to transmit the receipt to the digital folder based on an expense classification of the receipt matching the expense classification of the digital folder.

Patentansprüche

1. Verfahren, umfassend:

Erstellen, durch eine Verbrauchervorrichtung, eines digitalen Ordners auf der Grundlage einer Ausgabenklassifizierung in einem Dateiverwaltungssystem;
 Erzeugen, durch die Verbrauchervorrichtung, eines Schlüssels (212, 312) für eine Transaktion, wobei der Schlüssel (212, 312) eine zufällig erzeugte Zahl umfasst, die auf einer Eins-zu-Eins-Basis mit dem digitalen Ordner verbunden ist;
 Anzeigen, durch die Verbrauchervorrichtung, des Schlüssels (212, 312) auf einem Bildschirm der Verbrauchervorrichtung;
 Übertragen, durch die Verbrauchervorrichtung, des Schlüssels (212, 312) für eine Transaktion an eine Empfangsvorrichtung (110, 210, 310);
 Übertragen, durch die Verbrauchervorrichtung, der zufällig erzeugten Zahl an das Dateiverwaltungssystem; und
 eine Händlervorrichtung anweisen, durch das Verbrauchervorrichtung und über das Dateiverwaltungssystem, einen Beleg an den digitalen Ordner zu übertragen;

wobei die Händlervorrichtung den auf dem Bildschirm der Verbrauchervorrichtung angezeigten Schlüssel (212, 312) abtastet; und
 wobei, als Reaktion auf das Abtasten des Schlüssels (212, 312) durch die Händlervorrichtung, die Händlervorrichtung so konfiguriert ist, dass sie den Beleg auf der Grundlage einer Übereinstimmung der Ausgabenklassifizierung des Belegs mit der Ausgabenklassifizierung des digitalen Ordners, an den digitalen Ordner überträgt.

2. Verfahren nach Anspruch 1, wobei der Schlüssel (212, 312) mindestens eines von einem QR-Code oder einem Barcode umfasst.

3. Verfahren nach Anspruch 1, ferner umfassend das Übertragen, durch die Verbrauchervorrichtung, einer Anfrage zum Zugriff auf den Beleg, an das Dateiverwaltungssystem.

4. Verfahren nach Anspruch 3, wobei die Anfrage die zufällig erzeugte Zahl einschließt.

5. Verfahren nach Anspruch 1, ferner umfassend die Anzeige, durch die Verbrauchervorrichtung, des Belegs auf dem Bildschirm der Verbrauchervorrichtung.

6. Verfahren nach Anspruch 1, wobei das Dateiverwaltungssystem ein Cloud-Computing-System umfasst.

7. System umfassend:

einen Prozessor in einer Verbrauchervorrichtung,
 einen greifbaren, nicht flüchtigen Speicher, der zur Kommunikation mit dem Prozessor konfiguriert ist,
 den greifbaren, nicht flüchtigen Speicher, in dem Anweisungen gespeichert sind, die als Reaktion auf deren Ausführung durch den Prozessor, den Prozessor veranlassen, Arbeitsschritte durchzuführen, die Folgendes umfassen:

Erstellen, durch die Verbrauchervorrichtung, eines digitalen Ordners auf der Grundlage einer Ausgabenklassifizierung in einem Dateiverwaltungssystem;
 Erzeugen, durch die Verbrauchervorrichtung, eines Schlüssels (212, 312) für eine Transaktion, wobei der Schlüssel (212, 312) eine zufällig erzeugte Zahl umfasst, die auf einer Eins-zu-Eins-Basis mit dem digitalen Ordner verbunden ist;
 Anzeigen, durch die Verbrauchervorrichtung, des Schlüssels (212, 312) auf einem

- Bildschirm der Verbrauchervorrichtung;
Übertragen, durch die Verbrauchervorrichtung, des Schlüssels (212, 312) für eine Transaktion an eine Empfangsvorrichtung;
Übertragen, durch die Verbrauchervorrichtung, der zufällig erzeugten Zahl an das Dateiverwaltungssystem; und
eine Händlervorrichtung anweisen, durch die Verbrauchervorrichtung und über das Dateiverwaltungssystem, einen Beleg an den digitalen Ordner zu übertragen;
wobei die Händlervorrichtung den auf dem Bildschirm der Verbrauchervorrichtung angezeigten Schlüssel (212, 312) abtastet; und
wobei die Händlervorrichtung als Reaktion auf das Abtasten des Schlüssels (212, 312) durch die Händlervorrichtung so konfiguriert ist, dass sie den Beleg an den digitalen Ordner auf der Grundlage der Übereinstimmung einer Ausgabenklassifizierung des Belegs mit der Ausgabenklassifizierung des digitalen Ordners übereinstimmt, überträgt.
8. System nach Anspruch 7, wobei der Schlüssel (212, 312) mindestens eines von einem QR-Code oder einem Barcode umfasst.
9. System nach Anspruch 7, wobei die Arbeitsschritte ferner das Übertragen, durch die Verbrauchervorrichtung, einer Anfrage zum Zugriff auf den Beleg an das Dateiverwaltungssystem umfassen.
10. System nach Anspruch 9, wobei die Anfrage die zufällig erzeugte Zahl einschließt.
11. System nach Anspruch 7, wobei die Arbeitsschritte ferner die Anzeige, durch die Verbrauchervorrichtung, des Belegs auf dem Bildschirm der Verbrauchervorrichtung umfassen.
12. System nach Anspruch 7, wobei das Dateiverwaltungssystem ein Cloud-Computing-System umfasst.
13. Herstellungserzeugnis, das ein nichtflüchtiges, greifbares, computerlesbares Speichermedium mit darauf gespeicherten Anweisungen einschließt, die, als Antwort auf deren Ausführung durch eine Verbrauchervorrichtung, die Verbrauchervorrichtung veranlassen, Arbeitsschritte durzuführen, die Folgendes umfassen:
- Erstellen, durch die Verbrauchervorrichtung, eines digitalen Ordners auf der Grundlage einer Ausgabenklassifizierung in einem Dateiverwaltungssystem;

Erzeugen, durch die Verbrauchervorrichtung, eines Schlüssels (212, 312) für eine Transaktion, wobei der Schlüssel (212, 312) eine zufällig erzeugte Zahl umfasst, die auf einer Eins-zu-Eins-Basis mit dem digitalen Ordner verbunden ist;

Anzeigen, durch die Verbrauchervorrichtung, des Schlüssels (212, 312) auf einem Bildschirm der Verbrauchervorrichtung;

Übertragen, durch die Verbrauchervorrichtung, des Schlüssels (212, 312) für eine Transaktion an eine Empfangsvorrichtung;

Übertragen, durch die Verbrauchervorrichtung, der zufällig erzeugten Zahl an das Dateiverwaltungssystem; und

eine Händlervorrichtung anweisen, durch die Verbrauchervorrichtung und über das Dateiverwaltungssystem, einen Beleg an den digitalen Ordner zu übertragen;

wobei die Händlervorrichtung den auf dem Bildschirm der Verbrauchervorrichtung angezeigten Schlüssel (212, 312) abtastet; und

wobei die Händlervorrichtung, als Reaktion auf das Abtasten des Schlüssels (212, 312) durch die Händlervorrichtung, so konfiguriert ist, dass sie den Beleg an den digitalen Ordner auf der Grundlage der Übereinstimmung einer Ausgabenklassifizierung des Belegs mit der Ausgabenklassifizierung des digitalen Ordners übereinstimmt, überträgt.

Revendications

1. Procédé comprenant :

la création, par un dispositif consommateur, d'un dossier numérique basé sur une classification de dépenses dans un système de gestion de fichiers ;

la génération, par le dispositif consommateur, d'une clé (212, 312) pour une transaction, dans lequel la clé (212, 312) comprend un nombre généré aléatoirement associé de manière individualisée au dossier numérique,

l'affichage, par le dispositif consommateur, de la clé (212, 312) sur un écran du dispositif consommateur ;

la transmission, par le dispositif consommateur, de la clé (212, 312) à un dispositif de réception (110, 210, 310) pour une transaction ;

la transmission, par le dispositif consommateur, du nombre généré aléatoirement au système de gestion de fichiers ; et

l'instruction, par le dispositif consommateur et par le biais du système de gestion de fichiers, à un dispositif marchand de transmettre un reçu au dossier numérique ;

- dans lequel le dispositif marchand scanne la clé (212, 312) affichée sur l'écran du dispositif consommateur ; et
 dans lequel, en réponse au scannage de la clé (212, 312) par le dispositif marchand, le dispositif marchand est configuré pour transmettre le reçu au dossier numérique sur la base d'une correspondance d'une classification de dépenses du reçu avec la classification de dépenses du dossier numérique. 5 10
2. Procédé selon la revendication 1, dans lequel la clé (212, 312) comprend au moins un parmi un code-barres matriciel ou un code-barres. 15
3. Procédé selon la revendication 1, comprenant en outre la transmission au système de gestion de fichiers, par le dispositif consommateur, d'une requête d'accès au reçu. 20
4. Procédé selon la revendication 3, dans lequel la requête inclut le nombre généré aléatoirement. 25
5. Procédé selon la revendication 1, comprenant en outre l'affichage, par le dispositif consommateur, du reçu sur l'écran du dispositif consommateur. 30
6. Procédé selon la revendication 1, dans lequel le système de gestion de fichiers comprend un système informatique en nuage. 35
7. Système comprenant :
 un processeur dans un dispositif consommateur,
 une mémoire tangible et non transitoire, configurée pour communiquer avec le processeur, la mémoire tangible et non transitoire présentant des instructions stockées en son sein qui, en réponse à leur exécution par le processeur, amènent le processeur à mettre en œuvre des opérations comprenant : 40
 la création, par le dispositif consommateur, d'un dossier numérique basé sur une classification de dépenses dans un système de gestion de fichiers ;
 la génération, par le dispositif consommateur, d'une clé (212, 312) pour une transaction, dans lequel la clé (212, 312) comprend un nombre généré aléatoirement associé de manière individualisée au dossier numérique, 45
 l'affichage, par le dispositif consommateur, de la clé (212, 312) sur un écran du dispositif consommateur ; 50
 la transmission, par le dispositif consommateur, de la clé (212, 312) à un dispositif de 55
- réception pour une transaction ;
 la transmission, par le dispositif consommateur, du nombre généré aléatoirement au système de gestion de fichiers ; et
 l'instruction, par le dispositif consommateur et par le biais du système de gestion de fichiers, à un dispositif marchand de transmettre un reçu au dossier numérique ;
 dans lequel le dispositif marchand scanne la clé (212, 312) affichée sur l'écran du dispositif consommateur ; et
 dans lequel, en réponse au scannage de la clé (212, 312) par le dispositif marchand, le dispositif marchand est configuré pour transmettre le reçu au dossier numérique sur la base du fait qu'une classification de dépenses du reçu corresponde à la classification de dépenses du dossier numérique.
8. Système selon la revendication 7, dans lequel la clé (212, 312) comprend au moins un parmi un code-barres matriciel ou un code-barres.
9. Système selon la revendication 7, les opérations comprenant en outre la transmission au système de gestion de fichiers, par le dispositif consommateur, d'une requête d'accès au reçu.
10. Système selon la revendication 9, dans lequel la requête inclut le nombre généré aléatoirement.
11. Système selon la revendication 7, les opérations comprenant en outre l'affichage, par le dispositif consommateur, du reçu sur l'écran du dispositif consommateur.
12. Système selon la revendication 7, dans lequel le système de gestion de fichiers comprend un système informatique en nuage.
13. Article manufacturé incluant un support de stockage tangible et non transitoire, lisible par ordinateur, présentant des instructions stockées en son sein qui, lorsqu'elles sont exécutées par un dispositif consommateur, amènent le dispositif consommateur à mettre en œuvre des opérations comprenant :
 la création, par le dispositif consommateur, d'un dossier numérique basé sur une classification de dépenses dans un système de gestion de fichiers ;
 la génération, par le dispositif consommateur, d'une clé (212, 312) pour une transaction, dans lequel la clé (212, 312) comprend un nombre généré aléatoirement associé de manière individualisée au dossier numérique,
 l'affichage, par le dispositif consommateur, de la clé (212, 312) sur un écran du dispositif

consommateur ;
la transmission, par le dispositif consommateur,
de la clé (212, 312) à un dispositif de réception
pour une transaction ;
la transmission, par le dispositif consommateur, 5
du nombre généré aléatoirement au système de
gestion de fichiers ; et
l'instruction, par le dispositif consommateur et
par le biais du système de gestion de fichiers, à
un dispositif marchand de transmettre un reçu 10
au dossier numérique ;
dans lequel le dispositif marchand scanne la clé
(212, 312) affichée sur l'écran du dispositif
consommateur ; et
dans lequel, en réponse au scannage de la clé 15
(212, 312) par le dispositif marchand, le dispo-
sitif marchand est configuré pour transmettre le
reçu au dossier numérique sur la base d'une
correspondance d'une classification de dépen-
ses du reçu avec la classification de dépenses 20
du dossier numérique.

25

30

35

40

45

50

55

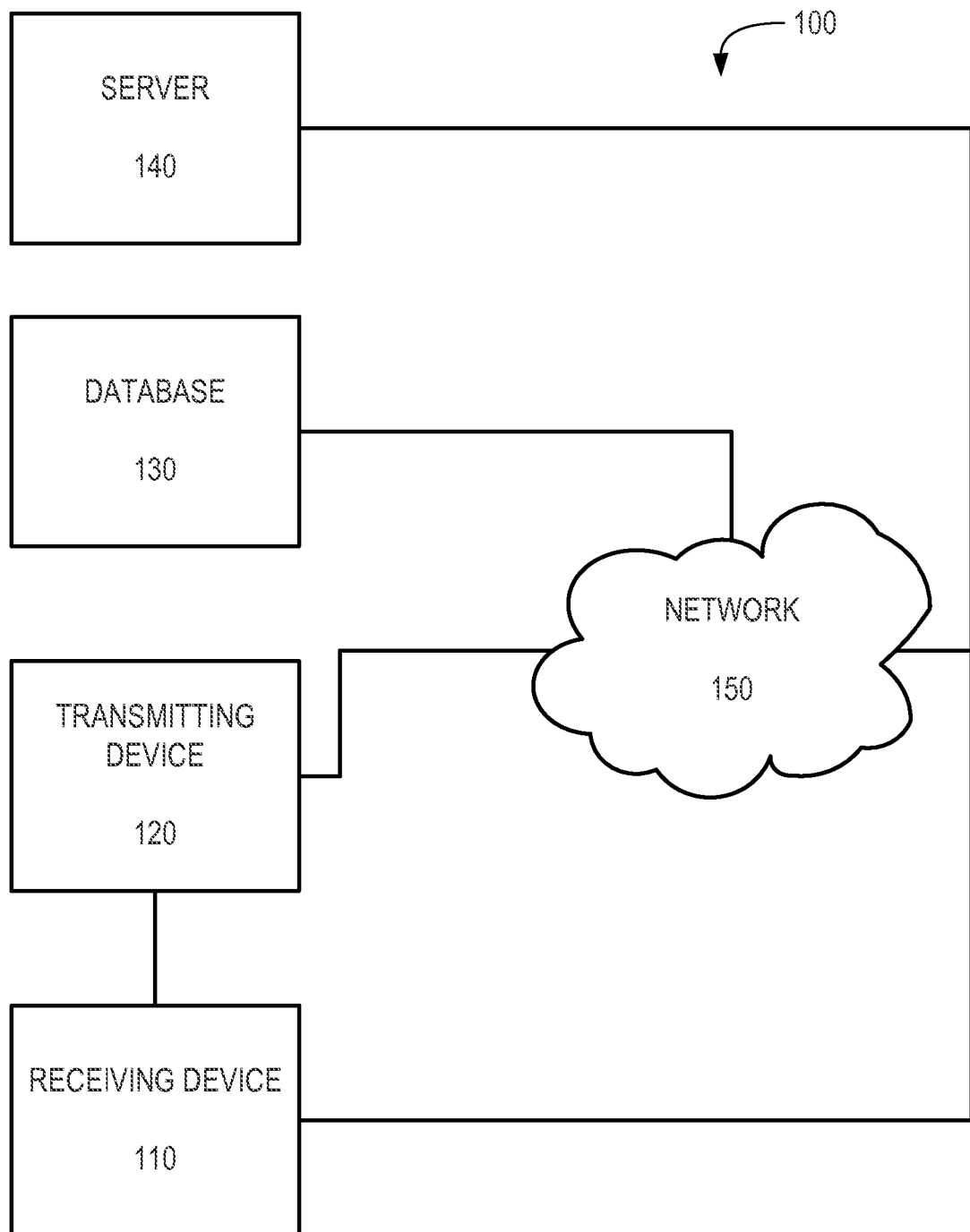


FIG. 1

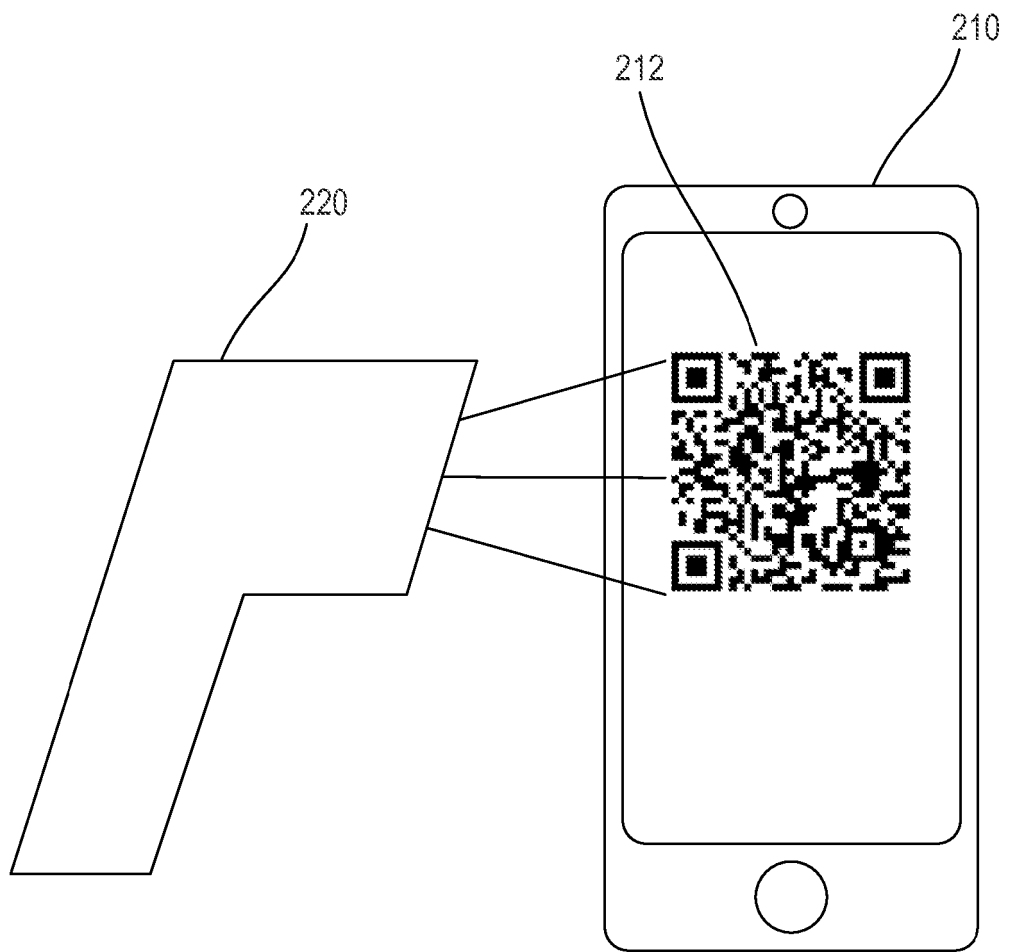


FIG. 2

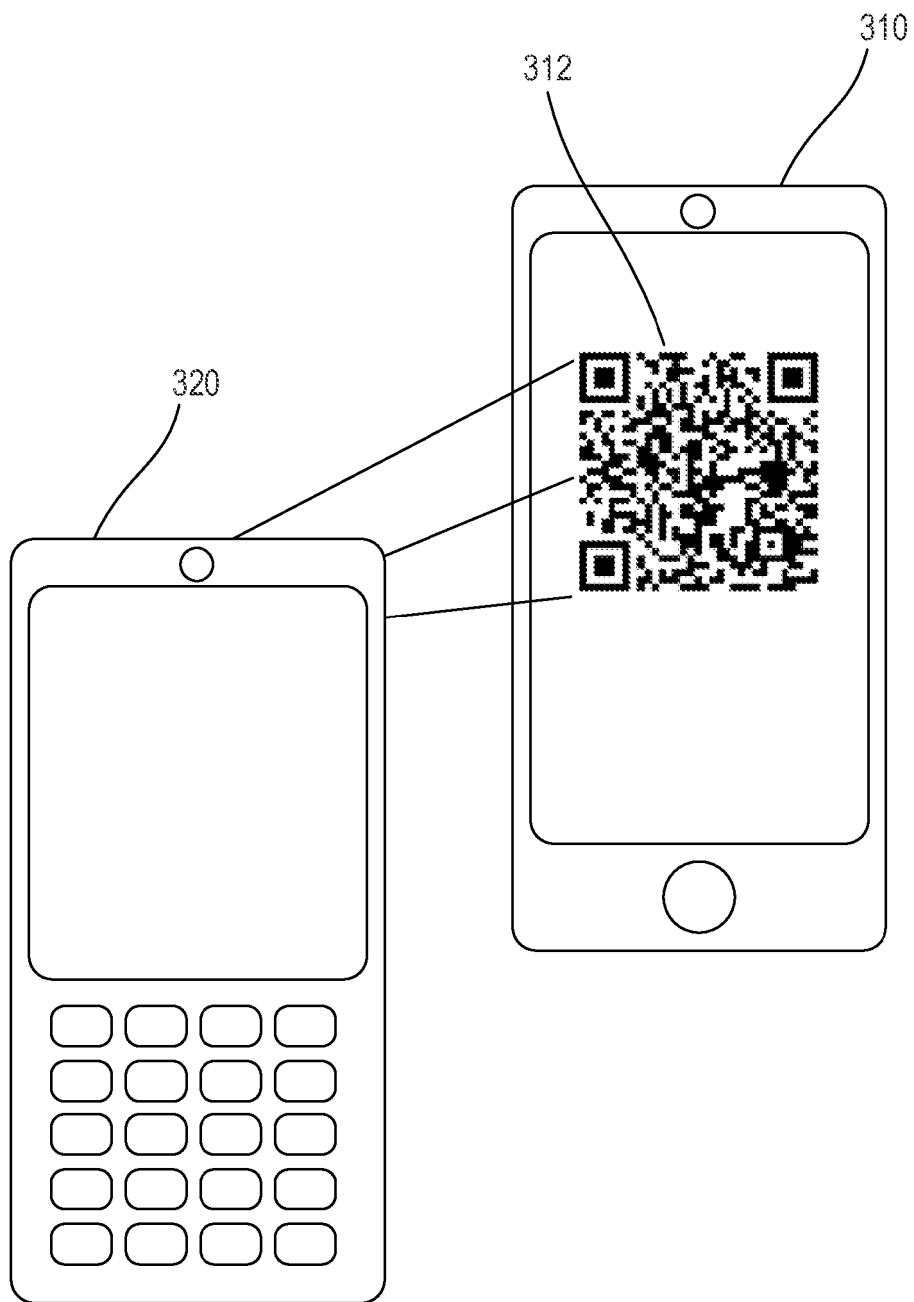


FIG. 3

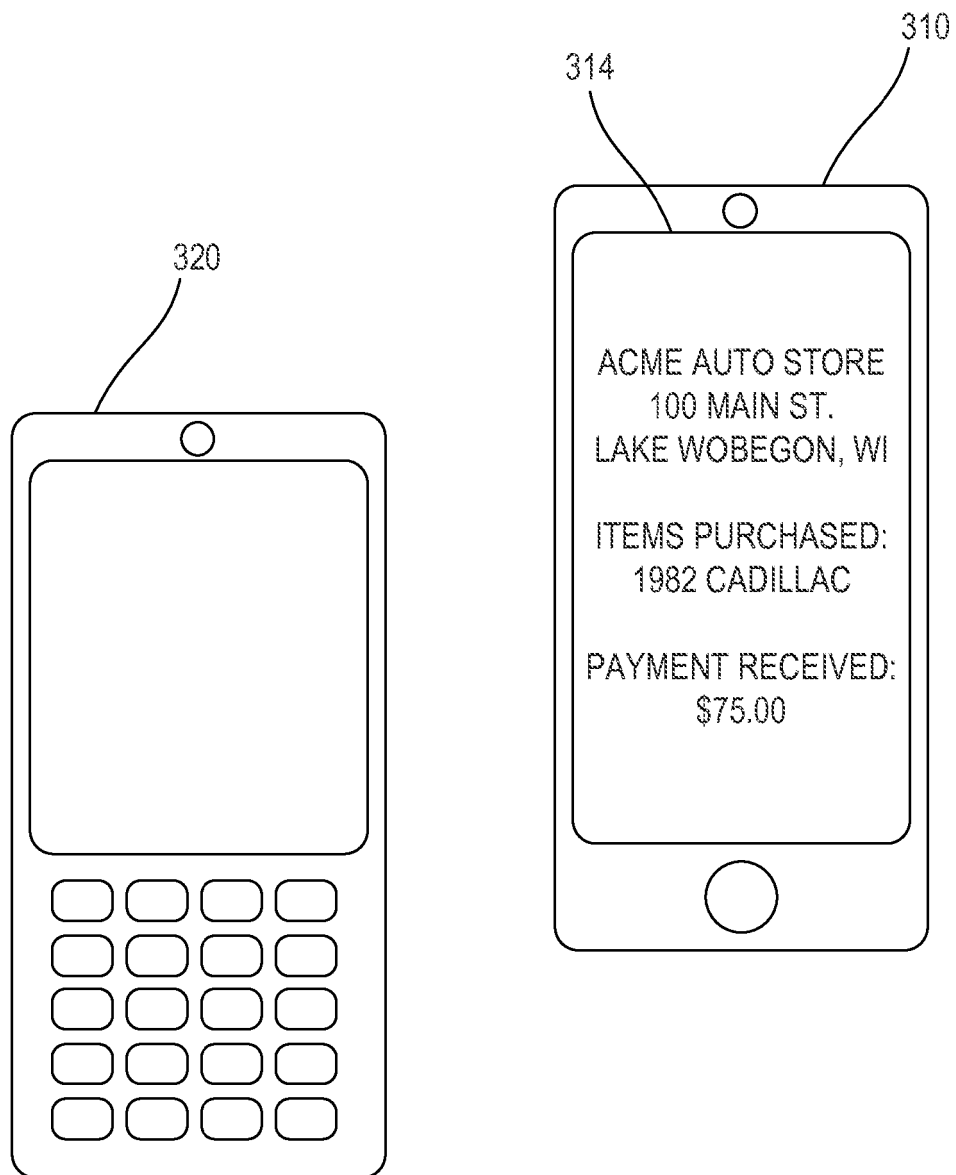


FIG. 4

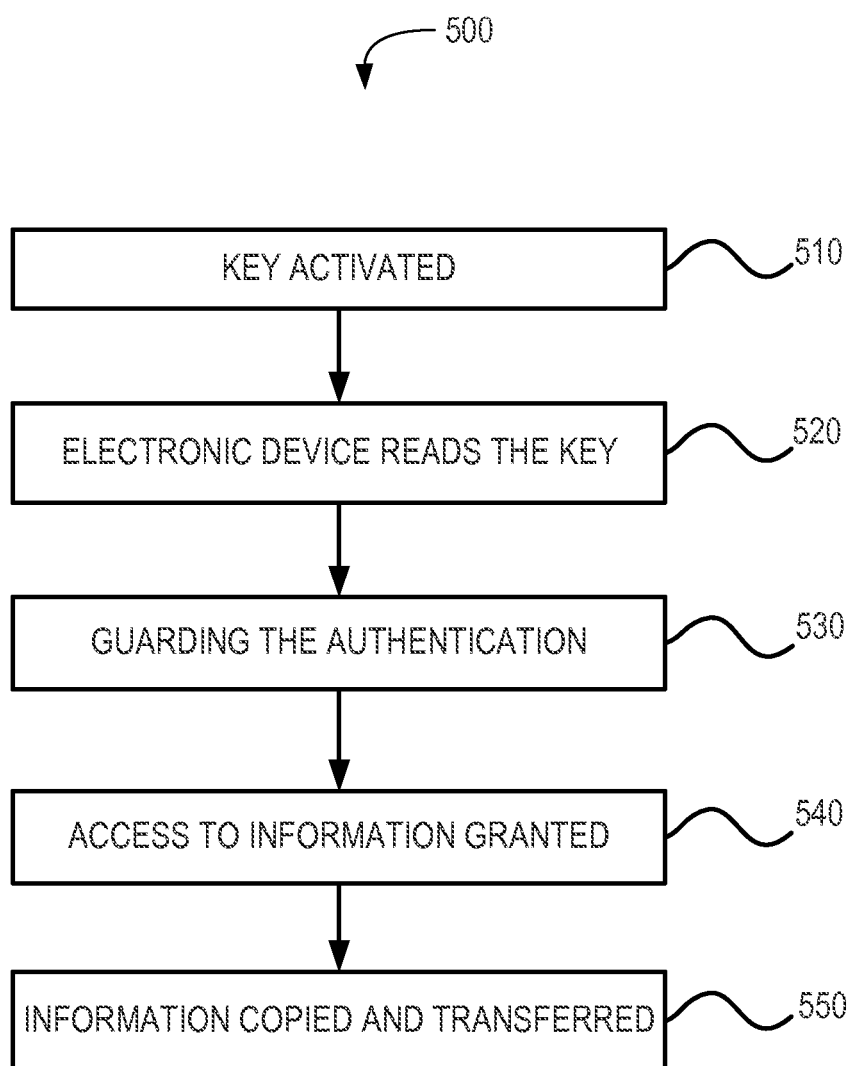


FIG. 5

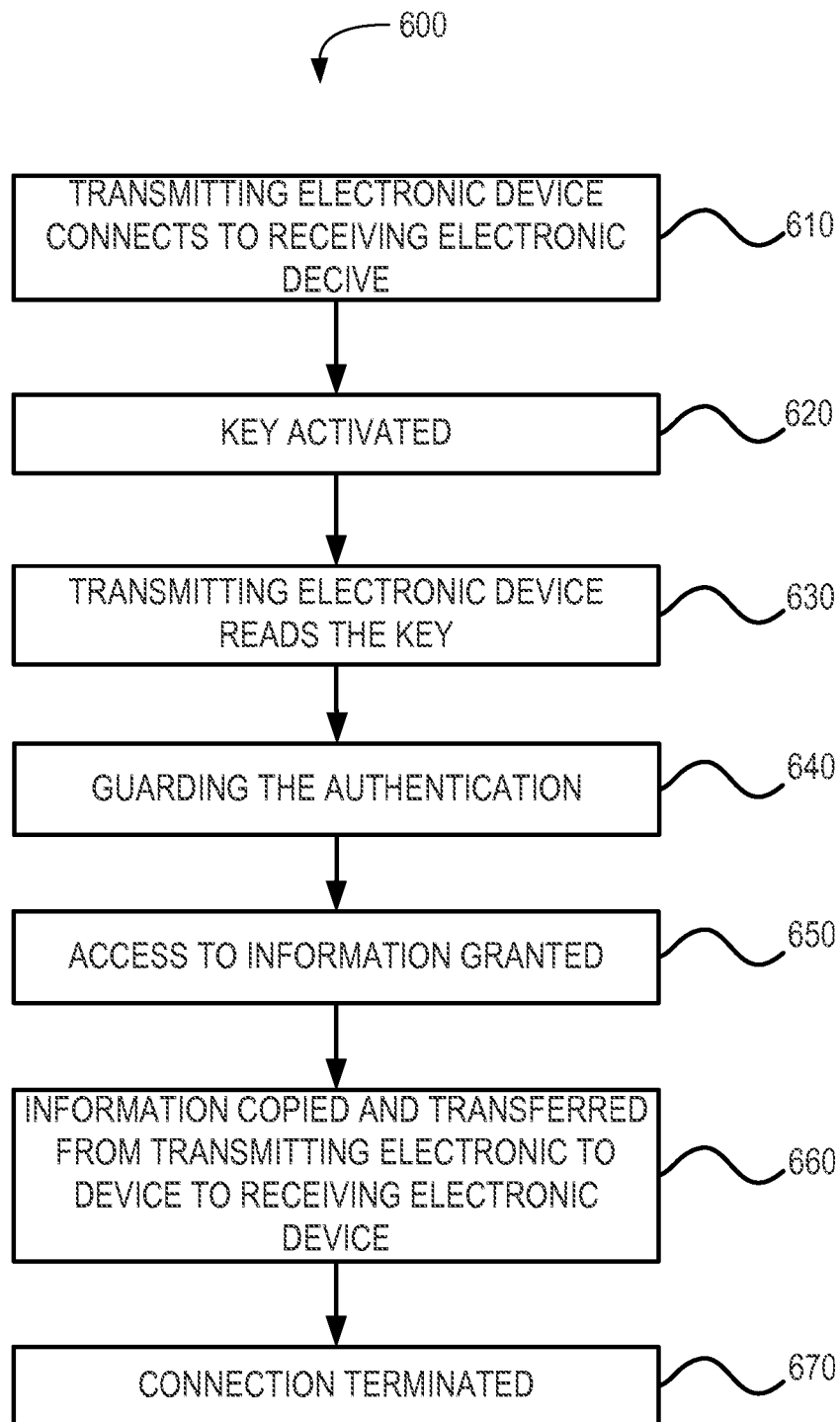


FIG. 6

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 103077462 A [0004]
- CN 102376133 A [0005]
- US 16491914 [0035]
- US 19751714 [0057]

Non-patent literature cited in the description

- **BRUCE SCHNEIER.** Applied Cryptography: Protocols, Algorithms, And Source Code In C. John Wiley & Sons, 1995 [0091]
- **JONATHAN KNUDSON.** Java Cryptography. O'Reilly & Associates, 1998 [0091]
- **WILLIAM STALLINGS.** Cryptography & Network Security: Principles & Practice. Prentice Hall [0091]